FRACTIONAL NUMBER-THEORETIC TRANSFORMS BASED ON MATRIX FUNCTIONS

Juliano B. Lima[1]*, Ricardo M. Campello de Souza*[2] *and Paulo Hugo E. S. Lima*[2]

Department of Mathematics[1], Department of Electronics and Systems[2]
Federal University of Pernambuco, Recife-PE, Brazil
e-mail: juliano_bandeira@ieee.org, ricardo@ufpe.br, paulohugos@gmail.com

ABSTRACT

In this paper, we introduce fractional number-theoretic transforms (FrNTT) based on matrix functions. The approach, which is a kind of finite field extension of the method presented in [1], does not require the construction of any number-theoretic transform eigenvector set. In this sense, the definition presented in this work is simpler than that of another recently introduced FrNTT. An image encryption scheme based on the proposed FrNTT is suggested.

Index Terms— Fractional transfoms, number-theoretic transforms, image encryption

1. INTRODUCTION

In the last years, fractional transforms have been used in applications related to different areas of knowledge. Such transforms can be viewed as generalizations of the corresponding ordinary transforms, where arbitrary powers of integral or matrix operators are computed [2]. The most well-known fractional transform is the fractional Fourier transform, the application of which to a signal can be interpreted as a rotation by an arbitrary angle in the time-frequency plane [3].

Recently, fractional number-theoretic transforms (FrNTT) have been introduced. Analogously to real-valued fractional transforms, FrNTT generalize number-theoretic transforms (NTT), which are computed over finite fields. More specifically, in [4], NTT are fractionalized by a method analogous to that presented in [5], which uses eigenvectors generated by complete generalized Legendre sequences; in [6], the authors follow the technique introduced in [7], which employs Hermite-Gaussian-like eigenvectors.

In this paper, we present a definition for fractional number-theoretic transforms analogous to that introduced in [1]. Our definition employs a technique based on matrix functions to compute arbitrary rational powers of an NTT matrix [8]. Concepts related to trigonometry in finite fields are also used [6, 9]. In comparison to previous approaches [4, 6], the proposed FrNTT has a simpler construction, since it is not necessary to obtain NTT eigenvectors. Similarly to other NTT, the computation of the FrNTT involves modular arithmetic only and can be carried out by standard fast algorithms. A scheme for image encryption based on the proposed FrNTT is suggested.

This paper is organized as follows. In Section 2, we review some concepts related to trigonometry in finite fields and number-theoretic transforms. In Section 3, the proposed FrNTT is introduced and an example is developed. In Section 4, an image encryption scheme based on the FrNTT is suggested; computer simulations and a security analysis are carried out. The paper closes with conclusions in Section 5.

2. PRELIMINARIES

In this section, we review some concepts related to trigonometry in finite fields. More details related to such concepts can be found in [6, 9]. We also present a definition for the number-theoretic transform and give its eigenvalues [4, 6].

Definition 1 *Let* $\mathrm{GF}(p)$ *be the finite field with* p *elements and* $\zeta \in \mathrm{GF}(p)$ *be an element with multiplicative order denoted by* $\mathrm{ord}(\zeta)$*. The finite field cosine and sine of the arc related to* ζ *are computed modulo* p*, respectively, as*

$$\cos_\zeta(x) := \frac{\zeta^x + \zeta^{-x}}{2} \quad \textit{and} \quad \sin_\zeta(x) := \frac{\zeta^x - \zeta^{-x}}{2\sqrt{-1}},$$

$x = 0, 1, \ldots, \mathrm{ord}(\zeta) - 1$.

Finite field cosines and sines hold properties similar to those of the standard real-valued ones. We also remark that, if $p \equiv 3 \pmod 4$, the number $-1 \pmod p$ is a quadratic nonresidue and, therefore, $\sqrt{-1} \pmod p$ lies in the extension field $\mathrm{GF}(p^2)$. This case is not considered in this paper.

Definition 2 *The number-theoretic transform of an* N*-length vector* $\mathbf{x} = (x_i)$*,* $x_i \in \mathrm{GF}(p)$*, is a vector* $\mathbf{X} = (X_k)$*,* $X_k \in \mathrm{GF}(p)$*, computed modulo* p *by*

$$X_k = \sqrt{N^{-1}} \sum_{i=0}^{N-1} x_i \zeta^{-ki}, \quad k = 0, 1, \ldots, N-1,$$

where $\zeta \in \mathrm{GF}(p)$ *and* $\mathrm{ord}(\zeta) = N$*. The inverse transform is*

$$x_i = \sqrt{N^{-1}} \sum_{k=0}^{N-1} X_k \zeta^{ki}.$$

978-1-4799-2893-4/14/$31.00 ©2014 IEEE

The relationship between $\mathbf{x}$ and $\mathbf{X}$ can be expressed by the matrix equation

$$\mathbf{X} = \mathbf{F}\mathbf{x},$$

where $\mathbf{F}$ is the transform matrix, the $(k+1)$-th row and $(i+1)$-th column element of which is given by $F_{k,i} = \sqrt{N^{-1}}\zeta^{-ki}$.

Proposition 1 *The* $\mathbf{F}$ *matrix has, at most, four distinct eigenvalues, namely* $\{1, -1, \sqrt{-1}, -\sqrt{-1}\}$*, computed in* $\mathrm{GF}(p)$.

3. FRACTIONAL NUMBER-THEORETIC TRANSFORM

In this section, we introduce a new definition for the fractional number-theoretic transform. The approach follows the idea originally presented in [1]. Differently from previous fractional NTT approaches [4, 6], the definition given here does not require the construction of NTT eigenvector sets. This simplifies the computation of the corresponding transform matrix, while the main properties required by a fractional transform are preserved.

The proposed definition is based on matrix functions [8], whose theory can be described using concepts which are valid also in the finite field scenario. Such concepts include, for example, the Lagrange interpolation polynomial for a given function and the minimal polynomial of a matrix [10]. Our goal is computing the function $\mathbf{F}^a$, where a is a rational number called *fractional parameter*. We start by considering the *minimal polynomial* of $\mathbf{A}$, which is defined as the unique monic polynomial ψ of lowest degree such that $\psi(\mathbf{A}) = 0$. The minimal polynomial divides any other polynomial r for which $r(\mathbf{A}) = 0$. According to the following theorem, $r(\mathbf{A})$ is completely determined by the values of r on the spectrum of $\mathbf{A}$.

Theorem 1 *Let* r *and* s *be polynomials and* $\mathbf{A}$ *be an* $N \times N$ *matrix over a finite field. Then* $r(\mathbf{A}) = s(\mathbf{A})$ *if and only if* r *and* s *take the same values on the spectrum of* $\mathbf{A}$.

The proof of Theorem 1 is analogous to that presented for Theorem 1.3 on page 5 of [8]. This result can be generalized to an arbitrary function f using the following definition.

Definition 3 *Let* f *be defined on the spectrum of an* $N \times N$ *matrix* $\mathbf{A}$ *over a finite field, and let* ψ *be the minimal polynomial of* $\mathbf{A}$*. Let* $\lambda_1, \ldots, \lambda_v$ *be the distinct eigenvalues of* $\mathbf{A}$ *and let* n_i *be the dimension of the largest Jordan block in which* λ_i *appears. Then* $f(\mathbf{A}) := r(\mathbf{A})$*, where* r *is the polynomial of degree less than* $\deg\psi$ *that satisfies the interpolation conditions*

$$r^{(j)}(\lambda_i) = f^{(j)}(\lambda_i), \quad j = 0, 1, \ldots, n_i - 1, \;\; i = 1, 2, \ldots, v.$$

If $n_i = 1$, $i = 1, \ldots, v$, r corresponds to the Lagrange interpolating polynomial [10]

$$r(t) = \sum_{i=1}^{v} f(\lambda_i) l_i(t), \quad l_i(t) = \prod_{j=1,\, j\neq i}^{v} \left(\frac{t - \lambda_j}{\lambda_i - \lambda_j}\right). \quad (1)$$

In order to employ Definiton 3 to compute $\mathbf{F}^a$, we set $f(t) = t^a$, where $a = a_1/a_2$ is a ratio of two integers. According to Proposition 1, one has $v = 4$, for $N > 4$, and $\lambda_1 = 1$, $\lambda_2 = -1$, $\lambda_3 = \sqrt{-1}$ and $\lambda_4 = -\sqrt{-1}$. We compute

$$l_1(t) = \frac{t^3 + t^2 + t + 1}{4},\; l_2(t) = \frac{-t^3 + t^2 - t + 1}{4},$$

$$l_3(t) = \frac{\sqrt{-1}t^3 - t^2 - \sqrt{-1}t + 1}{4},$$

$$l_4(t) = \frac{-\sqrt{-1}t^3 - t^2 + \sqrt{-1}t + 1}{4},$$

and, therefore,

$$r(t) = l_1(t) + (-1)^a l_2(t) + (\sqrt{-1})^a l_3(t) + (-\sqrt{-1})^a l_4(t).$$

From Equation (1), expressing $r(t) = t^a = t^{\frac{a_1}{a_2}}$ as

$$\sum_{i=0}^{3} \alpha_i(a) t^i = \sum_{i=0}^{3} \alpha_i(a_1, a_2) t^i,$$

one has

$$\begin{aligned}\alpha_0(a) = \alpha_0(a_1, a_2) =& \frac{1 + (\sqrt{-1})^a + (-1)^a + (-\sqrt{-1})^a}{4} \\ =& \frac{1}{4}\left\{\left(\sqrt[2a_2]{-1}\right)^{a_1}\left[1 + \left(\sqrt[2a_2]{-1}\right)^{a_1}\right] + \right. \\ &\left. + \left(\sqrt[2a_2]{-1}\right)^{-a_1}\left[1 + \left(\sqrt[2a_2]{-1}\right)^{a_1}\right]\right\} \\ =& \frac{1 + \left(\sqrt[2a_2]{-1}\right)^{a_1}}{2} \cos_{\sqrt[2a_2]{-1}}(a_1).\end{aligned}$$

Analogously, we obtain

$$\alpha_1(a_1, a_2) = \frac{1 - \sqrt{-1}\left(\sqrt[2a_2]{-1}\right)^{a_1}}{2} \sin_{\sqrt[2a_2]{-1}}(a_1),$$

$$\alpha_2(a_1, a_2) = \frac{-1 + \left(\sqrt[2a_2]{-1}\right)^{a_1}}{2} \cos_{\sqrt[2a_2]{-1}}(a_1)$$

and

$$\alpha_3(a_1, a_2) = \frac{-1 - \sqrt{-1}\left(\sqrt[2a_2]{-1}\right)^{a_1}}{2} \sin_{\sqrt[2a_2]{-1}}(a_1).$$

Finally, using Definition 3, we compute

$$\mathbf{F}^a = \mathbf{F}^{\frac{a_1}{a_2}} = r(\mathbf{F}) = \sum_{i=0}^{3} \alpha_i(a_1, a_2)\mathbf{F}^i. \quad (2)$$

Equation (2) corresponds to the matrix of the fractional number-theoretic transform with fractional parameter $a = a_1/a_2$. If $\mathbf{F}$ has dimensions $N \times N$, the FrNTT of an N-length vector $\mathbf{x}$ with components in a finite field is computed by

$$\mathbf{X}_a = \mathbf{F}^a\mathbf{x}. \quad (3)$$

3.1. Example

Let us construct an 8-point FrNTT over $\mathrm{GF}(257)$. We choose the element $\zeta = 4$, the multiplicative order of which is $N = \mathrm{ord}(4) = 8$. Using Definition 2, we obtain

$$\mathbf{F} = \begin{bmatrix} 242 & 242 & 242 & 242 & 242 & 242 & 242 & 242 \\ 242 & 197 & 17 & 68 & 15 & 60 & 240 & 189 \\ 242 & 17 & 15 & 240 & 242 & 17 & 15 & 240 \\ 242 & 68 & 240 & 197 & 15 & 189 & 17 & 60 \\ 242 & 15 & 242 & 15 & 242 & 15 & 242 & 15 \\ 242 & 60 & 17 & 189 & 15 & 197 & 240 & 68 \\ 242 & 240 & 15 & 17 & 242 & 240 & 15 & 17 \\ 242 & 189 & 240 & 60 & 15 & 68 & 17 & 197 \end{bmatrix}.$$

As an example, let us consider $a = a_1/a_2 = 3/8$. In order to compute $\alpha_i(3, 8)$, $i = 0, \ldots, 3$, we need $\sqrt{-1} \equiv \sqrt{256} \equiv 16 \pmod{257}$, $\left(\sqrt[16]{-1}\right)^3 \equiv 60^3 \equiv 120 \pmod{257}$, $\cos_{60}(3) = 196$ and $\sin_{60}(3) = 188$. Using Equation (2), we compute

$$\mathbf{F}^{\frac{3}{8}} = 36\mathbf{F}^0 + 28\mathbf{F}^1 + 97\mathbf{F}^2 + 97\mathbf{F}^3$$

$$= \begin{bmatrix} 57 & 181 & 181 & 181 & 181 & 181 & 181 & 181 \\ 181 & 241 & 112 & 14 & 76 & 52 & 145 & 83 \\ 181 & 112 & 112 & 145 & 181 & 112 & 173 & 145 \\ 181 & 14 & 145 & 241 & 76 & 83 & 112 & 52 \\ 181 & 76 & 181 & 76 & 57 & 76 & 181 & 76 \\ 181 & 52 & 112 & 83 & 76 & 241 & 145 & 14 \\ 181 & 145 & 173 & 112 & 181 & 145 & 112 & 112 \\ 181 & 83 & 145 & 52 & 76 & 14 & 112 & 241 \end{bmatrix}.$$

4. IMAGE ENCRYPTION BASED ON THE FRNTT

Encryption schemes have been widely used in scenarios related to multimedia security. With respect to digital images, the purpose of such techniques is to *scramble* and *transform* the pixels, in order to modify its statistical properties and visual aspect [11]. Here, we propose an image encryption technique based on the FrNTT defined in Section 3.

The method employs the M-length vector of integers

$$\mathbf{a}_1 = (\, a_{1,0} \;,\; a_{1,1} \;,\; \ldots \;,\; a_{1,M-1} \,)$$

as secret-key. The encryption consists in computing the bidimensional FrNTT of $\mathbf{B}_i$, the i-th block of an image, according to

$$\mathbf{B}_i^{\frac{a_{1,i} \,(\mathrm{mod}\ M)}{a_2}} = \mathbf{F}^{\frac{a_{1,i} \,(\mathrm{mod}\ M)}{a_2}}\, \mathbf{B}_i\, \mathbf{F}^{\frac{a_{1,i} \,(\mathrm{mod}\ M)}{a_2}}. \qquad (4)$$

In Equation (4), the parameter a_2 is constant. The blocks are transformed in a serial manner, as shown in Figure 1; block $\mathbf{B}_{i+1}$ is processed only after block $\mathbf{B}_i$ is processed and substituted by its transformed version. This is strictly necessary because there is a superposition among pixels of adjacent blocks. In the figure, the blocks have dimensions 8×8 pixels; subsequent blocks are alternately highlighted with a gray shadow and with a dashed border line, in order to make clear the pixel superposition. Blocks in the right border of the image must be completed with pixels in the left border of the image and immediately below the current "row of blocks" (see block $\mathbf{B}_4$ in Figure 1).

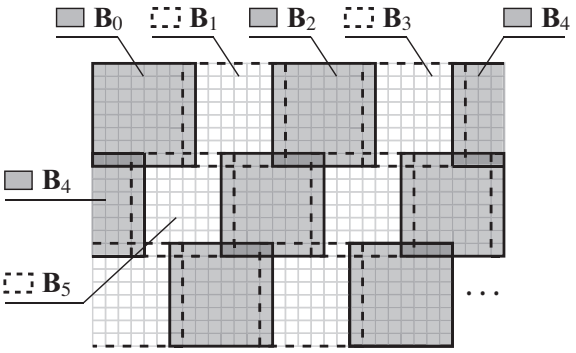

Fig. 1: Sequence of blocks to be processed in the image encryption scheme based on the FrNTT.

Two rounds of the encryption procedure are performed to obtain the final ciphered image. The decryption process consists in applying the encryption steps in reverse order. This includes the use of the fractional parameter $a = -\frac{a_{1,i} \,(\mathrm{mod}\ M)}{a_2}$ to compute the inverse FrNTT of the i-th image block.

4.1. Computer Simulations and Security Analysis

Simulations of the proposed encryption technique were performed using Matlab®. The grayscale images shown in the first row of Figure 2 were used. The images have dimensions 512×512 pixels and are encoded with 8 bits per pixel. We use the FrNTT developed in Example 1, with $a_2 = 64$ and a_1 taken from the 22-length secret-key

$$\mathbf{a}_1 = (53, 58, 9, 59, 41, 7, 18, 36, 62, 62, 11, 63, 62, 32, 52,$$
$$10, 27, 59, 51, 62, 2, 24)\,.$$

Once the transform is defined over $\mathrm{GF}(257)$, in order to avoid pixels equal to 256, each FrNTT is recursively applied to the corresponding image block until the maximum value of a pixel in a given block is 255. In this manner, the ciphered image can be encoded also with 8 bits per pixel. In the second row of Figure 2, the ciphered images are shown. We observe that the visual content of the images is completely noisy.

In Figure 3, the histograms of the original images and those of the corresponding ciphered images are shown. The application of the FrNTT leads to a uniformization of the histograms, which suggests that statistical attacks may not be feasible. The effectiveness of the encryption under statistical aspects can also be observed by computing the correlation between two adjacent pixels of the images [12]. In Table 1, we see that the original images have correlation coefficients close to 1; as expected, correlation coefficients of ciphered images are close to 0.

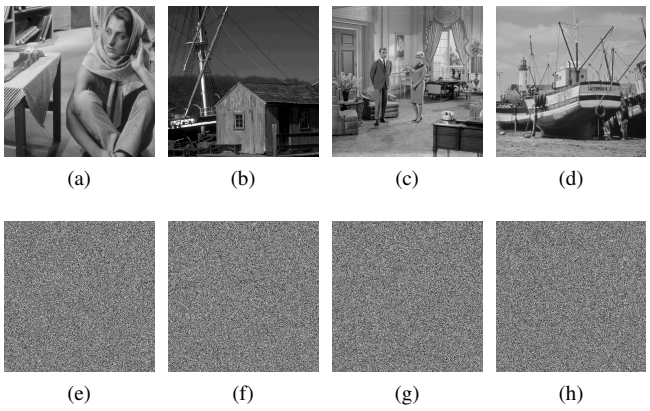

Fig. 2: Original and ciphered images. (a),(e) *img01.bmp*; (b),(f) *img02.bmp*; (c),(g) *img03.bmp*; (d),(h) *img04.bmp*.

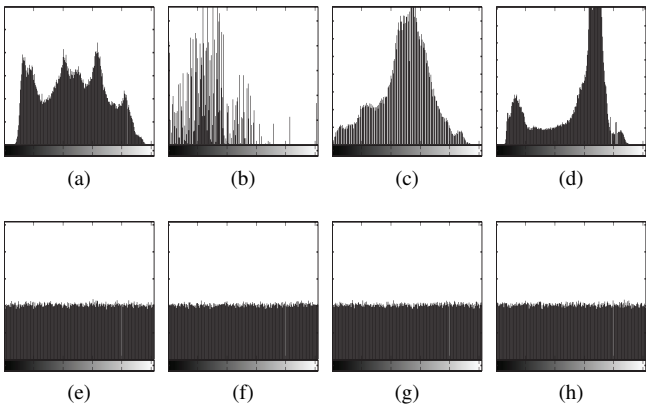

Fig. 3: Histograms of original and ciphered images. (a),(e) *img01.bmp*; (b),(f) *img02.bmp*; (c),(g) *img03.bmp*; (d),(h) *img04.bmp*.

In the simulations, the entropy of the ciphered images has assumed values varying from 7.9993 to 7.9994. This means that the transformed images are close to a random source and the proposed technique is also secure against the entropy attack [12]. Moreover, we see that the key space is sufficiently large to make brute-force attack unfeasible. Since $\mathbf{a}_1$ is a 22-dimensional vector whose elements are integers in the range $1-64$, we can assume that one has a 132-bit key. This satisfies the general requirement of resisting brute-force attack [13].

Finally, we analyze the key sensitivity of the proposed scheme by attempting to decrypt the ciphered images shown in Figure 2 using the key

$$\mathbf{a}_1' = (53, 58, 9, 59, 41, 7, 18, 36, 62, 62, 11, 63, 62, 32, 52,$$
$$10, 27, 59, 51, 62, 2, \underline{23})\,.$$

The *wrong* key $\mathbf{a}_1'$ differs from the correct key $\mathbf{a}_1$ only in 1 bit in the underlined position. We obtain the images shown in Figure 4. The noisy aspect of those images suggests that our method is highly sensitive to slight modifications in the key, which is desirable in cryptographic schemes.

Table 1: Correlation coefficients of the original images (r) and the corresponding ciphered images ($\tilde{r}$); (v), (h) and (d) are related to vertical, horizontal and diagonal correlation respectively. For each image, correlation coefficients were computed by using 2^{15} pairs of pixels randomly selected.

	r_h	$\tilde{r}_h$	r_v	$\tilde{r}_v$	r_d	$\tilde{r}_d$
img01	0.960	-0.001	0.897	-0.004	0.884	0.004
img02	0.936	-0.003	0.940	-0.004	0.889	-0.006
img03	0.953	0.008	0.946	0.004	0.911	0.015
img04	0.979	0.007	0.963	0.010	0.945	-0.009

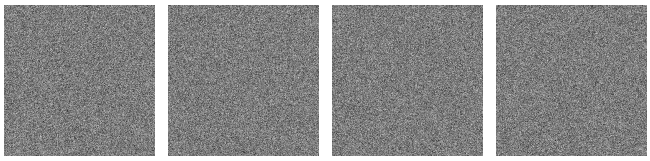

Fig. 4: Images decrypted with a key slightly different from the correct key. (a) *img01.bmp*; (b) *img02.bmp*; (c) *img03.bmp*; (d) *img04.bmp*.

5. CONCLUSIONS

In this paper, we have introduced a new definition for fractional number-theoretic transforms. Our approach is based on matrix functions and, in some sense, extends to the finite field scenario the discrete fractional Fourier transform presented in [1]. The proposed definition is simpler than those described in [4] and [6], once it does not involve the construction of orthonormal eigenvector sets of the corresponding NTT matrix. The FrNTT can be computed using standard fast algorithms and appears to be suitable for cryptographic purposes. Currently, we are investigating additional properties of the FrNTT and evaluating the possibility of using matrix functions to define other fractional transforms over finite fields.

6. REFERENCES

[1] B. Santhanam and J. H. McClellan, "The discrete rotational Fourier transform," *IEEE Transactions on Signal Processing*, vol. 44, no. 4, pp. 994–998, April 1996.

[2] E. Sejdić, I. Djurović, and L. Stanković, "Fractional Fourier transform as a signal processing tool: An overview of recent developments," *Signal Processing*, vol. 91, no. 6, pp. 1351–1369, June 2011.

[3] L. B. Almeida, "The fractional Fourier transform and time-frequency representations," *IEEE Transactions on Signal Processing*, vol. 42, no. 11, pp. 3084–3091, November 1994.

[4] S.-C. Pei, C.-C. Wen, and J. J. Ding, "Closed form orthogonal number theoretic transform eigenvectors and the fast fractional NTT," *IEEE Transactions on Signal Processing*, vol. 59, no. 5, pp. 2124–2135, May 2011.

[5] C.-C. Pei, S.-C. amd Wen and J. J. Ding, "Closed-form orthogonal eigenvectors generated by complete generalized Legendre sequences," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 55, no. 11, pp. 3469–3479, December 2008.

[6] J. B. Lima and R. M. Campello de Souza, "The fractional Fourier transform over finite fields," *Signal Processing*, vol. 92, no. 2, pp. 465–476, February 2012.

[7] C. Candan, M. Alper Kutay, and H. M. Ozaktas, "The discrete fractional Fourier transform," *IEEE Transactions on Signal Processing*, vol. 48, no. 5, pp. 1329–1337, May 2000.

[8] N. J. Higham, *Functions of Matrices: Theory and Computation*, Society for Industrial and Applied Mathematics, Philadelphia, 2008.

[9] R. M. Campello de Souza, H. M. de Oliveira, A.N. Kauffman, and A. J. A. Paschoal, "Trigonometry in finite fields and a new Hartley transform," in *Proc. IEEE Int. Symp. Information Theory (ISIT'98)*. IEEE, 1998, p. 293.

[10] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2nd edition, 2008.

[11] R. Tao, X.-Y. Meng, and Y. Wang, "Image encryption with multiorders of fractional Fourier transforms," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 4, pp. 734–738, December 2010.

[12] A. Akhshani, S. Behnia, A. Akhavan, H. Abu Hassan, and Z. Hassan, "A novel scheme for image encryption based on 2D piecewise chaotic maps," *Optics Communications*, vol. 283, no. 17, pp. 3259–3266, September 2010.

[13] Nigel Smart, "ECRYPT II yearly report on algorithms and keysizes (2010-2011)," Tech. Rep., European Network of Excellence in Cryptology II, 2011.